GUIDE SSI

Mettre en œuvre des moyens de défense minimums pour les connexions sans fil

mai 2005

Fiche 7

MEDEF

Accompagner

Cette fiche est complétée par la fiche n° 6 sur les moyens de défense minimums dans le cas des connexions fixes.

Qu'appelle-t-on « réseau sans fil » ?

C'est un moyen de connecter un terminal à un réseau (d'entreprise, Internet) sans utiliser de câblage physique.

Ces technologies sont également utilisées pour localement faire communiquer plusieurs terminaux entre eux sans avoir à créer de réseau permanent.

On classe les technologies sans fil selon leurs usages :

- **Les réseaux sans fil personnels** : ils permettent une connectivité entre appareils électroniques proches les uns des autres. Cet usage est aujourd'hui dominé par la technologie Bluetooth (portée typique de plusieurs mètres) ;

- **Les réseaux sans fil d'entreprise** : ils se substituent aux réseaux câblés d'entreprise classiques. La technologie la plus répandue est aujourd'hui le « Wi-Fi » (portée typique de quelques dizaines de mètres), utilisée soit intra-entreprise soit pour couvrir les zones d'affaires (« Hot-Spots »).

- **Les réseaux sans fil métropolitains** : ils permettent une couverture large (plusieurs dizaines de kilomètres) et sont utilisés le plus souvent pour proposer une connectivité à Internet en complément du câble ou de l'ADSL. Plusieurs technologies coexistent, parmi lesquelles le « WiMAX », soutenue par Intel qui l'intègrera dans sa future génération de microprocesseurs.

- **Les réseaux sans fil nationaux**, déployés par les opérateurs de téléphonie mobile, et dont les générations successives permettent de plus en plus de débit : GSM, GPRS, EDGE, UMTS. Ces deux dernières technologies, en cours de déploiement, amèneront des débits compatibles avec de véritables échanges de données d'entreprise.

Cette fiche envisage l'étude des deux technologies les plus répandues en entreprise aujourd'hui : le Bluetooth pour les réseaux sans fil personnels et le Wi-FI pour les réseaux sans fil d'entreprise.

Les vulnérabilités des réseaux sans fil

Les réseaux sans fil du type Wi-Fi ou Bluetooth offrent de multiples avantages : simplicité et coût modique d'installation, facilité d'usage, mobilité étendue. En contrepartie, ils sont par nature plus vulnérables aux attaques informatiques que les réseaux filaires.

Les principales vulnérabilités de ces réseaux sont les suivantes :

■ Les intrusions sur les réseaux ou les équipements connectés

Par définition, le cœur du réseau est accessible de l'extérieur par les équipements sans fil (ordinateurs équipés d'une interface radio, PDA ou téléphones portables dans le cas du Bluetooth). Il est extrêmement difficile de garantir que seules les personnes autorisées y auront accès. Ainsi une borne d'accès Wi-Fi porte en environnement dégagé à plus de 100 mètres, ce qui la rend le plus souvent atteignable bien au-delà du strict périmètre physique de l'entreprise.

La sécurité reposera donc fondamentalement sur la qualité du contrôle d'accès logique mis en place.

■ L'interception des données échangées par voie hertzienne

Puisque les données sont transmises par voie radio, elles peuvent être écoutées par l'ensemble des personnes présentes dans la zone d'émission, ce qui peut permettre de capter des informations précieuses, mais surtout donner des renseignements utiles pour mettre en œuvre une attaque plus dangereuse : une intrusion sur le système d'information par exemple.

Les protocoles sans fils intègrent maintenant quasi systématiquement des moyens de chiffrement des communications permettant de se prémunir de ce type d'attaques.

Toutefois à ce jour cette vulnérabilité est accentuée par le fait que certaines technologies sans fil contiennent des failles de sécurité et que la fonction de chiffrement n'est pas toujours activée.

■ Les perturbations de services

Le but de ces attaques dites « en deni de service » est de perturber durant un certain temps le bon fonctionnement du système. Il peut s'agir de rendre la borne d'accès à un réseau sans fil indisponible ou – plus grave - de paralyser le réseau.

La plus simple et la plus efficace des attaques consiste simplement à brouiller au niveau physique le spectre utilisé pour parasiter les communications. La source est cependant aisément identifiable, et peut être neutralisée.

Une menace plus importante réside en une sollicitation indue de l'équipement sans fil - des demandes de connexion multiples par exemple - qui peut saturer les entrées et ainsi interdire tout accès aux utilisateurs légitimes, mais aussi engendrer d'autres dysfonctionnements sur les réseaux connectés. La parade résidera dans l'architecture de sécurité mise en place derrière les points d'accès Wi-Fi, et la bonne configuration des équipements.

Si la disponibilité des services est la principale exigence de sécurité, le choix du sans fil n'est sans doute pas le plus judicieux.

La mise en œuvre de la sécurisation du sans fil

Les équipements sans fil étant accessibles le plus souvent au-delà du périmètre physique sécurisé de l'entreprise, il est indispensable de les sécuriser dès leur installation. De fait, la mise en œuvre d'un réseau Wi-Fi nécessite un niveau sécurité minimal, sans quoi l'entreprise sera une cible facile et privilégiée des pirates informatiques ou de la concurrence. Les principes généraux sont décrits ci-dessous pour deux environnements spécifiques : Bluetooth et Wi-Fi.

■ Sécurité des réseaux sans fil personnels (Bluetooth)

Bluetooth est une technologie de « souplesse ». La sécurité du protocole Bluetooth est - dans sa version actuelle - insuffisante pour garantir une résistance aux attaques évoluées. On évitera donc d'utiliser cette technologie pour connecter des équipements supportant ou donnant accès à des informations d'une importance stratégique pour l'entreprise.

Par extension, il est fondamental de ne pas utiliser cette technologie pour des équipements du type PDA communiquant reliés eux-mêmes à des réseaux sensibles.

D'une façon générale, pour se prémunir des intrusions et du vol de données sur les réseaux personnels utilisant Bluetooth, il convient de configurer correctement les équipements :

- ➔ en inhibant le mode découverte et appariement ;
- ➔ en activant la reconnaissance d'équipements répertoriés (par liste d'appareils « amis » autorisés) ;
- ➔ en activant le chiffrement des données ;
- ➔ en activant le mode invisible.

De plus, pour les équipements nomades (téléphone mobile ou PDA) intégrant une interface Bluetooth, les fonctions de liaison sans fil doivent être désactivées par défaut pour être réactivées lors d'un usage ponctuel. Ceci permet en particulier de se prémunir de certaines contaminations virales du type « ver bluetooth ».

■ Sécurité des réseaux sans fils d'entreprise (Wi-Fi)

La sécurité d'un réseau local sans fil de type Wi-Fi est plus complexe et peut être réalisée à différents niveaux. Elle intègre l'ensemble des préconisations de sécurité valables pour un réseau filaire (c.f. fiche 6) plus un ensemble de préconisations spécifiques au sans fil.

Compte tenu de la difficulté pour restreindre l'accès à un réseau sans fil, il est indispensable d'associer à son déploiement une procédure spécifique de sécurité.

Au delà de la formation et de la sensibilisation des utilisateurs cette étape comprend a minima :

- **la configuration des couches liaison et transport**
- **la gestion des accès**
- **les mises à jour logicielles**
- **l'audit périodique et la surveillance active de son réseau.**

Le tableau suivant récapitule la démarche minimum de sécurisation d'un réseau Wi-Fi :

- Sécuriser les points d'accès, les clients Wi-Fi et le compte administrateur et utiliser une liste d'accès d'appareils autorisés.

- S'assurer que les mécanismes de sécurité intégrés et normalisés sont bien activés (authentification, chiffrement WPA (Wi-Fi Protected Access) ou WPA2, liste d'équipements autorisés). La conservation de la configuration par défaut des équipements Wi-Fi est aujourd'hui la principale cause de compromission ; elle est donc à bannir.

- Mettre à jour le logiciel des équipements Wi-Fi (nouvelles versions logicielles qui corrigent les failles de sécurité).

- Etendre (et compléter) les services de sécurité déjà déployés sur le réseau filaire (exemple par VPN, firewall…).

- Mettre en œuvre les outils et règles d'authentification et les politiques de sécurité.

- Différencier les utilisateurs Wi-Fi une fois qu'ils sont connectés.

- Informer et former les utilisateurs. Pour les appareils en mobilité, les fonctions de liaison sans fil Wi-Fi doivent être désactivées par défaut et réactivées pour un usage ponctuel.

- Auditer le réseau : Un audit physique (s'assurer que le réseau sans fil ne diffuse pas d'informations dans des zones non désirées et qu'il n'existe pas de réseau sans fil non désiré dans le périmètre à sécuriser) et un audit informatique (s'assurer que le degré de sécurité obtenu est bien égal à celui désiré).

- Surveiller le réseau : surveillance au niveau IP avec un système de détection d'intrusions classique et surveillance au niveau physique (sans fil) avec des outils dédiés.